A Deep Learning Assisted Cryptographic Scheme Integrating Graph Neural Networks and Convolutional Autoencoders for Secure Data Transmission

A. V. Gahan
School of Electronics and Communication Engineering, REVA University, Bengaluru, India
gahanbit@gmail.com (corresponding author)

Geetha D. Devanagavi
School of Computer Science and Engineering, REVA University, Bengaluru, India
dgeetha@reva.edu.in

Received: 6 February 2026 | Revised: 26 February 2026 and 15 March 2026 | Accepted: 26 March 2026

 DOI: https://doi.org/10.48084/etasr.18023

ABSTRACT

Advanced Encryption Standard (AES-256) is a cryptographic algorithm that offers high confidentiality under standard security assumptions. However, structured data inherently possess correlations before encryption. This study proposes a structural and statistical pre-processing framework that uses Graph Neural Networks (GNNs) and Convolutional Autoencoders (CAEs) to transform the structured plaintext data before performing AES-256 encryption. The plaintext data are first converted into a graph structure to represent their inter-block relationships. The GNN learns the relational embeddings, which are further compressed by a CAE into low-dimensional latent spaces. These new spaces are subsequently encrypted using AES-256 without changing their internal architecture. The cryptographic security of the system is entirely inherited from AES-256, while the proposed learning-based module functions as a deterministic pre-processing transformation applied before encryption. The experimental results on computational complexity and statistical diffusion properties demonstrated consistency with statistical diffusion properties and computational efficiency, without compromising the security guarantees of AES-256.

Keywords-secured cryptography; graph neural networks; convolutional autoencoders; deep learning–based security; intelligent encryption

I. INTRODUCTION

The rise of networked systems, cloud computing, the Internet of Things (IoT), automotive networks, and wireless communications has made secure data transmission a necessity [1]. Cryptography is significant for information security as it ensures data privacy, integrity, authenticity, and non-repudiation [2, 22]. However, sophisticated cyber-attacks, large-scale data exchange, and the advent of quantum computing are posing new difficulties to established cryptography systems [3]. Thus, research has focused on integrating data preprocessing techniques to prepare the data before the encryption process, which helps handle relational data in the modern communication environment [20]. Authors in [21] examined the potential of deploying Machine Learning (ML) techniques to apply structural or statistical transformations to the data before they are encrypted, without changing the basic primitive of the cryptographic tool. Conventional cryptographic systems, including symmetric key algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), asymmetric key algorithms such as RSA and ECC, and hash functions (SHA family) [23], have established good security guarantees under certain computational assumptions [4]. Nonetheless, these systems frequently rely on static keys, predetermined mathematical assumptions, and set security parameters, rendering them susceptible to side-channel attacks, key compromise, brute-force attacks, and cryptanalytic advances [5]. With the rising complexity of attack vectors, current cryptography incorporates adaptive, intelligent, and hybrid security mechanisms [6]. These security mechanisms include ML and Deep Learning (DL) models for dynamic key generation, intrusion-aware encryption, anomaly detection, and attack prediction [7, 24]. Neural networks can learn complicated patterns in data traffic and cryptographic activities, allowing for proactive defensive systems to modify encryption strength and key management procedures in real time [8, 25]. These intelligent cryptographic frameworks greatly enhance resilience to zero-day attacks and advanced persistent threats [9]. Another important aspect of safe cryptography is post-quantum cryptography, which

overcomes the weaknesses introduced by quantum computers [10, 26]. Quantum algorithms, such as Shor's and Grover's algorithms, compromise the security of commonly used public-key cryptosystems by significantly lowering the computing effort necessary to solve factorization and discrete logarithm problems [11]. Post-quantum cryptography addresses these issues by providing lattice-based [27], code-based, hash-based, and multivariate polynomial encryption systems [28], ensuring long-term security in a post-quantum world [12, 29].

The present study proposes a Graph Neural Network (GNN)-Convolutional Autoencoder (CAE) module as a structural transformation layer before encryption. The proposed GNN-CAE framework allows relational feature extraction and representation compression without modifying the internal operations of the cryptographic algorithm. GNN-CAE is designed to perform relational feature extraction and statistical decorrelation while preserving the cryptographic security guarantees of AES-256. Although traditional cryptographic methods provide data confidentiality, they have limitations in terms of robustness, adaptability, and efficiency, especially when dealing with structured data and image-based applications.

TABLE I. SUMMARY OF RELATED WORK IN CRYPTOGRAPHIC AND ML-ASSISTED SECURITY METHODS

Study	Methodology adopted	Merits	Key limitations
[13]	Analytical study of relationships among major cryptographic algorithms such as AES and RSA.	Identifies security trade-offs and algorithm dependencies.	Primarily theoretical; lacks experimental implementation or performance evaluation.
[14]	Hybrid scheme integrating AES-256 with additional processing for secure encryption.	Improves integrity protection and encryption efficiency.	Extra processing increases computational cost.
[15]	Neural-assisted encryption (IHNC) using ML-based transformations before encryption.	Enhances feature hiding and diffusion characteristics.	Requires model training and higher implementation complexity.
[16]	ML-based secure routing using clustering, XGBoost aggregation, and optimized encryption.	Supports efficient and secure communication in sensor networks.	Multi-stage design increases system complexity.
[17]	Lightweight proxy signature using hyperelliptic curve cryptography.	Reduces computation and communication overhead.	Requires specialized cryptographic implementation and parameter selection.
[30]	Comparative analysis of lightweight cryptographic protocols for IoMT devices.	Highlights energy-efficient authentication solutions.	Focuses on comparison instead of a new security architecture.

Emerging modern communication technologies, including IoT and blockchain, depend on structured and correlated data. Traditional cryptographic algorithms, such as AES, have strong formal security guarantees; however, these algorithms are applied directly over the plaintext without considering the underlying correlated structure present in the structured data. In many real-world problems, data blocks need to be correlated before the actual encryption. To address this issue, the present study employs GNNs for data decorrelation, followed by the application of CAEs for efficient data representation before the AES-256 encryption.

II. METHODOLOGY

The proposed framework provides a learning-based pre-processing pipeline to transform the structured plaintext data before encryption. Figure 1 illustrates the workflow of the proposed GNN-CAE cryptographic system. The input data from the dataset are first subjected to entropy-based block-level preprocessing, where each image is normalized, partitioned into blocks, and statistical properties such as entropy are extracted to represent the data [18, 19]. The embeddings are then encoded using a CAE, resulting in a compact latent representation that improves obfuscation and removes redundancy. The latent features are then protected employing a cryptographic layer that uses AES and RSA encryption.

A. Input Data

The Proposed GNN-CAE method uses the BOSSBase v1.01 dataset [31] as input data. It is a widely recognized benchmark dataset in digital image cryptography/,which is developed to facilitate standardized evaluation of cryptographic security. The dataset consists of 20,000 images, each with a resolution of 512×512 pixels.

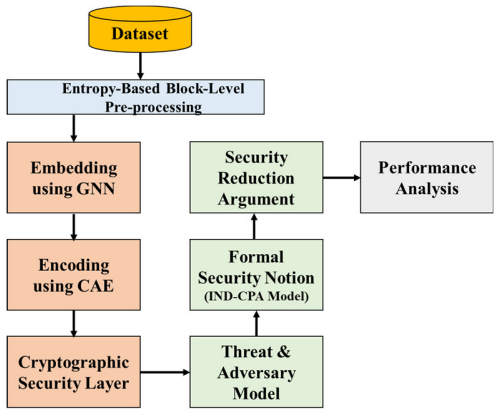

Fig. 1. Architecture of the proposed GNN-CAE framework.

At the initial stage, the sender's original unencrypted data are used as the system input. At this point, the data are raw and unencrypted, making them susceptible to interception or unauthorized access, as shown in:

$$X = \{x_1, x_2, x_3, \ldots, x_N\} \quad (1)$$

where X represents a collection of supplied plaintext data, and N is the total number of data blocks.

B. Entropy–Based Statistical Preprocessing with Block-Level Normalization

The pre-processing stage includes normalization, block segmentation, and entropy-based statistical feature extraction, as shown in Figure 2.

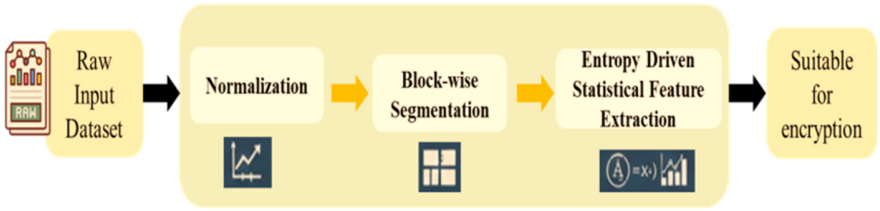

Fig. 2. Architecture of Entrophy –based statistical preprocessing with block-level normalization.

In the normalization step, the values are normalized to a specific range, while block segmentation is performed to capture local structural characteristics. Shannon entropy is computed on each block to measure statistical variability before its representation as a graph. In the proposed framework, each block is associated with an entropy value, which captures the levels of unpredictability within the input data. The entropy value indicates the level of uniformity with which the associated values are distributed in each block of the input data, such that the blocks with high entropy values have high levels of unpredictability associated with the input data. This is advantageous when implementing the theory in cryptographic applications. The pre-processing transformation and Shannon entropy computation are defined as:

$$X' = P(X) \quad (2)$$

$$H(x_i) = -\sum_{j=1}^{M} p_{ij} log_2(p_{ij}) \quad (3)$$

where X′ denotes the pre-processed data, $P(\cdot)$ is the pre-processing function, $H(x_i)$ represents the entropy of the blockx_i, $p_{ij}$is the probability j^{th} of the symbol in the block x_i, and $M$is the number of distinct symbols. The process eliminates redundancy and yields structured representations that are applicable for graph-based learning before encryption.

C. GNN-Driven Secure Embedding Generation

The pre-processed data are then represented as a graph, where the vertices are represented by blocks, and the edges denote the relational dependencies between the blocks. This representation enables modeling the contextual relationships that do not exist between independent blocks. Figure 3 shows the embedding layer of the GNN, which safely embeds the nodes of the GNN by aggregating information from the neighboring blocks. Equation (4) captures the entire graph representation that underlies the pre-processed data, showing how plaintext data are transformed into an entire graphical data type to enable GNN exploitation. Equation (5) defines the node feature vector. Equation (6) captures an overview of how node embeddings are updated within this entire GNN data embedding layer. It captures the message-passing mechanism, where each node updates its representation by aggregating information from its neighbors.

$$G = (V, E) \quad (4)$$

Each node in the graph represents a data block and begins with a feature vector, which is defined as:

$$x_v = [\mu, \sigma^2, H, PCA(v)] \quad (5)$$

where μ is the mean intensity of the block, σ^2 is the variance, H is the Shannon entropy, and $PCA(v)$ is the flattened block after dimension reduction. The entropy is only used as a feature and does not affect the pixel values or the AES-256 security.

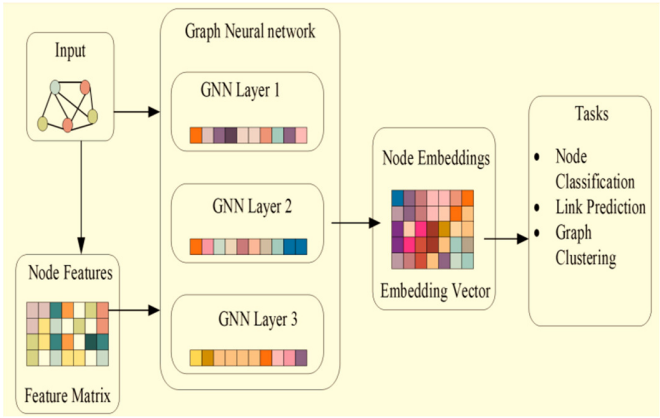

Fig. 3. Architecture of GNN-based secure embedding generation.

The initialization method considers both the local statistics and the structural information, which are informative embeddings for GNNs.

$$h_v^{(k)} = \sigma(W^{(k)} \cdot \sum_{u \in N(v)} h_u^{(k-1)} + b^{(k)}) \quad (6)$$

where G is the graph representation of the data, V denotes the set of nodes (data blocks), E is a set of edges (relationships), $h_v^{(k)}$ is the embedding of the node v at layer k, $N(v)$ is the neighbor set of the node v, $W^{(k)}$is the trainable weight matrix, and $b^{(k)}$ is the bias vector.

D. Latent Feature Encoding via CAE

The GNN embeddings are further processed using a CAE to obtain a compact latent representation that is suitable for encryption. This process reduces redundancy and enhances data obfuscation, resulting in a more secure representation. Figure 4 illustrates the architecture for/of latent feature encoding via CAE.

The encoding operation performed by the CAE on the embeddings generated by the GNN is given by:

$$Z_{latent} = f_{enc}(Z_{GNN}) \quad (7)$$

where Z_{latent} is the latent encoded representation, f_{enc} is the encoder function, and Z_{GNN} is the GNN output embeddings. This step compresses and decorrelates structural representations before encryption, enhancing the statistical diffusion properties of the resulting data.

E. Encryption Module for Secure Cipher Generation

The latent feature representation provided by the CAE model is further secured using the AES, a symmetric-key block cipher that exhibits excellent efficiency in terms of security.

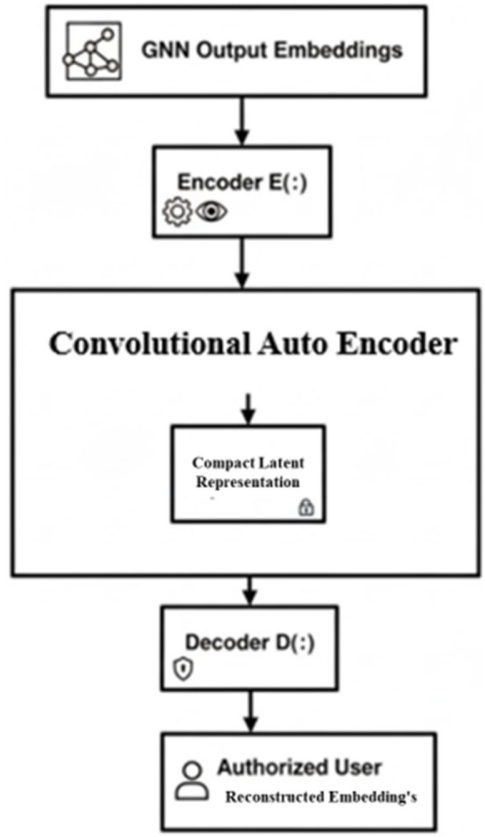

Fig. 4. Architecture of latent feature encoding via CAE.

The system utilizes AES with a 256-bit key length, referred to as AES-256. AES is a symmetric-key block cipher, which is used in Cipher Block Chaining (CBC) mode. Each time AES is used, it has a randomly generated 128-bit Initialization Vector (IV), which provides semantic security. The IV is generated by a cryptographically secure random number generator and sent with the ciphertext. To achieve secure key exchange, the AES session key is encrypted using the RSA algorithm in combination with Optimal Asymmetric Encryption Padding (OAEP), referred to as RSA-OAEP. OAEP ensures semantic security in the RSA encryption process and protects against chosen ciphertext attacks in the key encapsulation process. Once the key exchange is established, the sender uses AES-256, whereas the receiver utilizes the same in the context of decryption. At this stage, the classical cryptographic system is combined with confidence learned representation, providing structured representations that improve statistical diffusion properties before encryption. The hybrid encryption process used in the proposed system is defined as:

$$C = AES_K\left(Z_{latent}\right), K_{enc} = RSA_{K_{pub}}(K) \quad (8)$$

where Z_{latent} is the latent representation created by a CAE, K is the session key for AES-256 symmetric encryption, AES_K is the AES encryption function, $RSA_{K_{pub}}$ is the RSA encryption function using a receiver's public key, K_{enc} is the encrypted session key, and C is the final ciphertext created during the encryption process. The text to be converted into ciphertext is given as *C*, and the security of the system is dependent on the IND-CPA security of AES 256. The confidentiality of the resulting ciphertext is based solely on AES, assuming the standard IND-CPA security game. The learning-based pre-processing happens before the encryption, and it is a structural transformation tool that does not affect the cryptographic primitive.

F. Threat Model and Adversarial Assumptions

The proposed framework is evaluated using the conventional Dolev-Yao model of attack, where the attacker has complete control over the communication channel. The attacker can intercept, replay, inject, and modify the ciphertexts exchanged between the honest parties. In addition, the attacker is assumed to be computationally limited and runs in Probabilistic Polynomial Time (PPT). The study assumes a Chosen-Plaintext Attack (CPA) scenario where the attacker can adaptively query the encryption oracle with plaintexts of its choice and obtain the corresponding ciphertexts. The goal of the attacker is to distinguish the encryptions of two chosen plaintexts with non-negligible advantage. The security of the symmetric encryption phase is based on the conventional cryptographic assumption that AES-256 is a secure pseudorandom permutation when used in a semantically secure mode of operation. The RSA algorithm is solely used for key encapsulation and does not change the security assumptions of symmetric security.

1) Formal Security Notion (IND-CPA Model)

The proposed scheme is designed to achieve IND-CPA security, which refers to indistinguishability under chosen-plaintext attacks. Let us assume an adversary $\bar{A}$ playing the IND-CPA game. The model will proceed as:

1. $\bar{A}$ chooses two plaintexts X_0 and X_1 of equal length.
2. A random bit b is chosen from *{0, 1}*.
3. The challenger computes a ciphertext $C = Enc_K(T(X_b))$ and sends it to $\bar{A}$.
4. $\bar{A}$ then outputs a guess b'

The advantage of the adversary is defined as:

$$Adv_{\bar{A}}^{IND-CPA} = \left| Pr[b' = b] - \frac{1}{2} \right| \quad (9)$$

In the proposed scheme, the encryption algorithm can be expressed as:

$$C = AES_K\big(T(X)\big)$$

where $T(\cdot)$ is the deterministic preprocessing algorithm performed by the GNN-CAE module, and K is the AES-256 key.

2) Security Reduction Argument

Let the encryption procedure of the proposed system be given by (10). Where $T(\cdot)$is the deterministic pre-processing carried out by the GNN-CAE module. Let a probabilistic polynomial adversary $\bar{A}$, such that it is possible to violate the IND-CPA security of the proposed system with a non-negligible advantage. Then it is possible to construct an adversary using $\bar{A}$ to violate the IND-CPA security of the AES-256 cipher. The deterministic nature of the pre-processing $T(\cdot)$, not depending on the encryption key, enables the adversary to simulate the pre-processing and forward the pre-processed plaintext to the AES-256 challenger. Thus, any attack on the proposed framework implies an attack on the AES-256 cipher as well. Let the AES-256 cipher be IND-CPA secure. Then the proposed system is IND-CPA secure as well.

$$Enc_K(X) = AES_K\big(T(X)\big) \tag{10}$$

The IND-CPA security is tied to AES as:

$$Adv^{IND-CPA}_{Proposed}(\bar{A}) \leq Adv^{IND-CPA}_{AES}(\bar{A}) \tag{11}$$

Therefore, the overall cryptographic security of the proposed framework can be guaranteed by the security of AES-256 based on standard computational assumptions.

III. EXPERIMENTAL SETUP

The GNN-CAE-based cryptography framework was compared with MC [13], BF [14], IHNC [15], and AES-256 encryptions in MATLAB R2024a on an Intel Core i5 processor with 4 GB RAM under similar conditions. The BOSSBase v1.01 [31] dataset (20,000 grayscale images of 512 × 512 pixels) was used. The dataset was divided into training and testing sets utilizing an 80/20 split. Images were normalized to [0,1] for 16 × 16 non-overlapping blocks, yielding 1024 blocks per image. Shannon entropy, block mean, variance, and PCA-reduced pixels were used as node features, with edges represented by a 4-neighborhood adjacency matrix. A two-layer graph convolutional network produced 128- and 64-dimensional node embeddings, followed by a CAE (two 3 × 3 convolutional layers with 32 and 64 filters, 128-dimensional latent space, ReLU activation functions, and sigmoid output). Training was performed using the Adam optimizer (learning rate = 0.001, batch size = 32, 100 epochs) with Mean Squared Error (MSE) loss and L2 regularization. The latent features were fed into AES-256 encryption without changing its architecture. Ablation analysis (AES-only, GNN-only, CAE-only, GNN-CAE + AES-256) revealed that AES-256 provides cryptographic security, while the GNN-CAE modules carry out the structural transformation and decorrelation of features before the encryption process. The effectiveness of the transformation is also quantitatively measured by the diffusion measures, such as entropy, Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), and the avalanche effect, as well as the performance measures of execution time and throughput.

A. Baseline Methods

To evaluate the proposed GNN-CAE pre-processing approach, experiments were carried out on standalone AES-256, MC [13], BF [14], and IHNC [15] encryptions. AES-256 is considered the primary baseline because of its formal security proof for IND-CPA security and conventional symmetric encryption approach. The comparison of the pre-processing step to the direct AES encryption process helps in determining whether the pre-processing step has any effect on statistical diffusion or computational complexity. MC encryption [13] is a structurally improved cryptographic design, BF [14] is a hybrid encryption scheme, and IHNC [15] is a neural-assisted cryptographic benchmark. These baselines ensure a systematic comparison of diffusion properties, including entropy, NPCR, UACI, and avalanche effect, as well as efficiency metrics, such as execution time and throughput, while maintaining the same level of security.

IV. RESULTS AND DISCUSSION

The performance evaluation of the proposed GNN–CAE-based framework was conducted using metrics, including NPCR, UACI, avalanche effect, throughput, entropy, and execution time analysis.

A. Execution Time Analysis

Execution time represents the overall time required for encryption and decryption, and is given by:

$$ET = \sum_{i=1}^{N} X_i \times (T_{encryption} + T_{decryption}) \tag{12}$$

where X_i is the plaintext, $T_{encryption}$ denotes the encryption time, and $T_{decryption}$ is the decryption time.

Figure 5 compares the execution time for the proposed GNN-CAE approach with AES-256, MC, BF, and IHNC encryption algorithms for varying sample sizes (2,000-20,000 messages). The execution time is slightly affected by the addition of a new pre-processing stage. Nevertheless, it is observed that the overhead introduced by the GNN–CAE module is very low, amounting to only 2-3 ms compared to standalone AES-256 encryption. The execution time analysis proves that the additional GNN-CAE pre-processing step has a small computational cost compared to the standalone AES-256. This small computational cost is sustained by the fact that the pre-processing is done on compressed features.

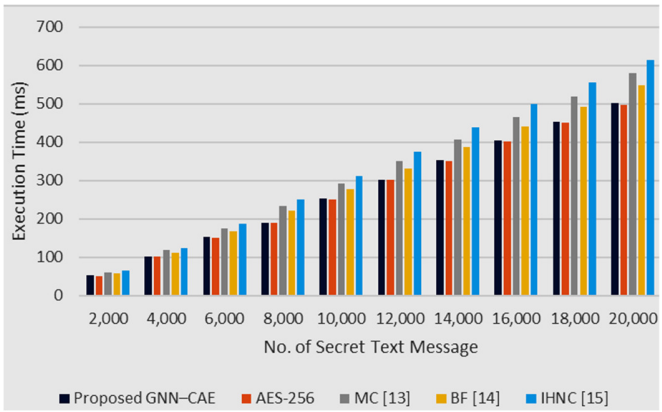

Fig. 5. Execution time comparison of the proposed GNN-CAE-based secured cryptography framework with AES-256, MC [13], BF [14], and IHNC [15] encryptions.

B. Throughput Analysis

The efficiency of the proposed framework is evaluated using throughput analysis. Throughput measures the rate at which data are encrypted and decrypted over a given period of time, and is defined as:

$$TP = \frac{\sum_{i=1}^{N} D_i}{T_{total}} \quad (13)$$

where D_i is the size of the i^{th} processed data block, N is the total number of blocks, and T_{total} is the total execution time.

Figure 6 displays the throughput performance of the proposed GNN-CAE framework in comparison to AES-256, MC [13], BF [14], and IHNC [15] encryptions with varying amounts of data. The experimental results show that the proposed framework has efficient throughput performance for varying data sizes. The slight differences in throughput performance for large data sizes can be attributed to the additional computational complexity of the proposed framework in the graph formation, GNN message passing, and CAE encoding processes. Throughput results indicate that the proposed framework maintains stable performance across varying data sizes despite the additional preprocessing stage.

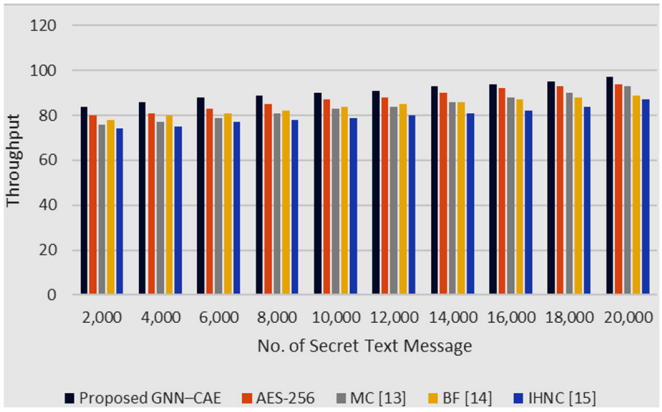

Fig. 6. Throughput comparison of the proposed GNN-CAE-based secured cryptography system with AES-256, MC [13], BF [14], and IHNC [15] encryptions.

C. Entropy Analysis

Entropy is used in this work as a statistical randomness measure of the ciphertext distribution. As the proposed system is expected to produce near-uniform ciphertext distributions under standard security assumptions, high entropy values are expected by design. Thus, the interpretation of entropy values is based on statistical diffusion properties rather than their use as formal proof of enhanced cryptographic security. The difference in randomness between the plaintext and the ciphertext is calculated using the entropy difference formula:

$$\Delta H = H(C) - H(X) \quad (14)$$

where $H(C)$ is the entropy of the ciphertext and $H(X)$ is the entropy of the plaintext. A positive ΔH value indicates an increase in statistical dispersion, while a value close to zero indicates that the statistical dispersion characteristics remain similar. Similarly, negative values indicate a decrease in dispersion. However, AES-256 already has near-uniform distributions of the ciphertext; hence, the entropy analysis is mainly focused on the statistical diffusion characteristics of the preprocessing and transformation phase.

Figure 7 illustrates the entropy comparison results for different methods. For different data sizes, the GNN-CAE pre-processing results in transformed input data with consistent statistical diffusion properties before encryption. This implies the consistency of the diffusion properties of the transformed input data before encryption, for different sizes of data. The main differences between the methods are the variations of the structural pre-processing, rather than the cryptographic primitive. Since all methods use the same AES-256 encryption method, the security level is the same under the threat model. Since the AES-256 encryption method already results in a uniform distribution of the ciphertexts, the results are only an interpretation of the structural changes.

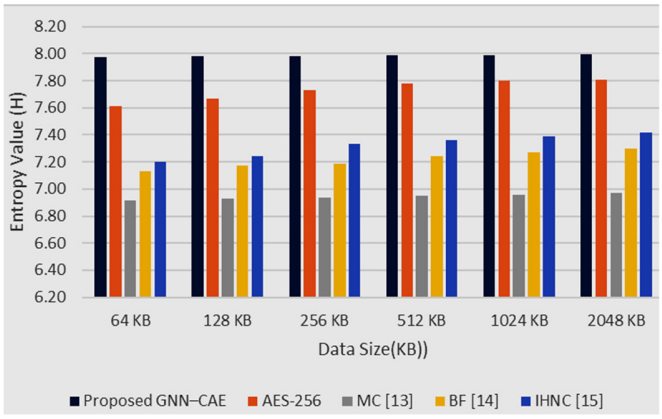

Fig. 7. Entropy comparison of the proposed GNN-CAE-based secured cryptography system with AES-256, MC [13], BF [14], and IHNC [15] encryptions.

D. NPCR, UACI, and Avalanche Effect Analysis

The diffusion and sensitivity of the proposed GNN-CAE-based encryption framework are analyzed using NPCR, UACI, and the avalanche effect. NPCR is used to measure the percentage of ciphertext elements that change when a single element in the plaintext is varied, as expressed in (15). UACI is used to measure the average intensity of change in the ciphertext due to variations in the plaintext, as shown in (16). The avalanche effect is used to measure the percentage of ciphertext bits that change when a single input bit is varied, as expressed in (17). The proposed framework has better diffusion properties as indicated by the enhanced values of NPCR and UACI, as well as the closeness of the entropy values to the theoretical limits. This implies that minor variations of the plaintext are propagated to a large portion of the ciphertext.

$$NPCR(\%) = \frac{Number\ of\ changed\ elements\ in\ ciphertext}{Total\ number\ of\ elements} \times 100 \quad (15)$$

$$UACI(\%) = \frac{Sum\ of\ absolute\ differences\ between\ ciphertexts}{Total\ number\ of\ elements\ \text{X}\ 255} \times 100 \quad (16)$$

$$avalanche\ effect\ (\%) = \frac{Number\ of\ changed\ bits\ in\ ciphertext}{Total\ Cipher\ Text\ bits} \times 100 \quad (17)$$

Table II compares the diffusion performance of the proposed method and existing encryption schemes using NPCR, UACI, and the avalanche effect. For this comparison, a single bit of the plaintext is varied, and the resulting input is passed through the GNN + CAE pre-processing phase and AES-256 encryption. NPCR, UACI, and avalanche effect are calculated by comparing the original and varied ciphertexts. The proposed approach is compared with AES-256 standalone, MC [13], BF [14], and IHNC [15] encryptions. The proposed framework has better NPCR and UACI values compared to the existing approaches, which represent the diffusion and sensitivity of the approaches. The avalanche effect value is close to the ideal value of 50%, which indicates that small variations in the input result in the effective diffusion of the variations throughout the ciphertext.

TABLE II. COMPARISON OF NPCR, UACI, AND AVALANCHE EFFECT FOR THE PROPOSED GNN–CAE-BASED CRYPTOGRAPHIC FRAMEWORK

Method	NPCR (%)	UACI (%)	Avalanche effect (%)
Proposed GNN-CAE	99.61	33.25	49.82
AES-256	99.26	32.90	49.10
MC [13]	98.78	31.40	48.30
BF [14]	98.92	32.05	48.70
IHNC [15]	98.85	31.80	48.50

V. CONCLUSION

This study proposed a structural and statistical pre-processing mechanism based on Graph Neural Networks (GNNs) and the Convolutional Autoencoders (CAE) for the transformation of the structured data prior to actual encryption using the Advanced Encryption Standard (AES-256) algorithm. The proposed mechanism transforms the structured data into a graphical structure and then learns the representations using the representation learning mechanism. The proposed pre-processing mechanism transforms the structured data without altering the internal encryption mechanism of the AES-256 algorithm; therefore, the security of the system remains the same as that of the AES algorithm under the IND-CPA model. The experimental results demonstrate the efficacy of the proposed mechanism in terms of stable throughput and execution time for various data sizes. Future work will include evaluating the framework on larger datasets, such as CIFAR-10 and ImageNet, implementing the model on hardware platforms, and checking the compatibility of the model with post-quantum cryptographic systems.

DECLARATION OF COMPETING INTERESTS

The authors declare no competing interests.

ACKNOWLEDGMENT

No external funding was received for this study.

DATA AVAILABILITY

The dataset used in this is publicly available and can be found in [31]. Any other data supporting the findings of this study are available from the corresponding author upon reasonable request.

AI USE AND DECLARATION OF GENERATIVE AI USE

The authors declare that no generative AI tools were used in this study.

REFERENCES

[1] M. A. Qasem *et al.*, "Cryptography Algorithms for Improving the Security of Cloud-Based Internet of Things," *SECURITY AND PRIVACY*, vol. 7, no. 4, Jul. 2024, Art. no. e378, https://doi.org/10.1002/spy2.378.

[2] R. Kaur and C. Sahu, "Cryptography in Industry," in *Next Generation Mechanisms for Data Encryption*, 1st ed., Boca Raton, FL, USA: CRC Press, 2024, pp. 146–163.

[3] R. A. Jowarder and S. Jahan, "Quantum Computing in Cyber Security: Emerging Threats, Mitigation Strategies, and Future Implications for Data Protection," *World Journal of Advanced Engineering Technology and Sciences*, vol. 13, no. 1, pp. 330–339, Sep. 2024, https://doi.org/10.30574/wjaets.2024.13.1.0421.

[4] P. Singh *et al.*, "Understanding RSA Algorithm in Cryptography," Undergraduate Thesis, University of Jammu, Jammu, India, 2024.

[5] P. Singh, P. Pranav, and S. Dutta, "Optimizing Cryptographic Protocols Against Side Channel Attacks Using WGAN-GP and Genetic Algorithms," *Scientific Reports*, vol. 15, no. 1, Jan. 2025, Art. no. 2130, https://doi.org/10.1038/s41598-025-86118-4.

[6] A. I. Saiyed, "Hybrid Quantum-Classical Cryptographic Protocols: Enhancing Security in the Era of Quantum Supremacy," *Spectrum of Research*, vol. 5, no. 1, pp. 1–7, 2025.

[7] S. Fu, H. Xu, A. Ali, and S. Sajid, "PriFed-IDS: A Privacy-Preserving Federated Reinforcement Learning Framework for Secure and Intelligent Intrusion Detection in Digital Health Systems," *Electronics*, vol. 14, no. 23, Nov. 2025, Art. no. 4590, https://doi.org/10.3390/electronics14234590.

[8] N. Fazrina, "Securing Distributed Sensor Systems Through Adaptive Encryption Algorithms in 5G-Based Smart Energy Networks," *Open Journal of Robotics, Autonomous Decision-Making, and Human-Machine Interaction*, vol. 9, no. 11, pp. 18–27, 2024.

[9] M. Khule, D. Motwani, and D. Chauhan, "A Layered and Integrative Framework for Advance Persistent Threat Detection and Mitigation: Combining AI, Zero-Trust, and Advanced Threat Intelligence," *Cluster Computing*, vol. 28, no. 11, Oct. 2025, Art. no. 740, https://doi.org/10.1007/s10586-025-05561-0.

[10] K. Mansoor, M. Afzal, W. Iqbal, and Y. Abbas, "Securing the Future: Exploring Post-Quantum Cryptography for Authentication and User Privacy in IoT Devices," *Cluster Computing*, vol. 28, no. 2, Apr. 2025, Art. no. 93, https://doi.org/10.1007/s10586-024-04799-4.

[11] Y. Ding, F. Tan, Z. Qin, M. Cao, K.-K. R. Choo, and Z. Qin, "DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption." arXiv, 2020, https://doi.org/10.48550/ARXIV.2012.11097.

[12] G. S. Mamatha, N. Dimri, and R. Sinha, "Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era." arXiv, 2024, https://doi.org/10.48550/ARXIV.2403.11741.

[13] C. Benitez, "Mapping Quantum Threats: An Engineering Inventory of Cryptographic Dependencies." arXiv, Mar. 03, 2026, https://doi.org/10.48550/arXiv.2509.24623.

[14] H. E. Mozo, "Quantum-Classical Hybrid Encryption Framework Based on Simulated BB84 and AES-256: Design and Experimental Evaluation." Jun. 27, 2025, https://doi.org/10.36227/techrxiv.175099973.38232383/v1.

[15] A. Badr, "Instant-Hybrid Neural-Cryptography (IHNC) Based on Fast Machine Learning," *Neural Computing and Applications*, vol. 34, no.

22, pp. 19953–19972, Nov. 2022, https://doi.org/10.1007/s00521-022-07539-0.

[16] R. Devendiran and A. V. Turukmane, "A Secured Cryptographic Approach with Extreme Gradient Boosting Model for Data Aggregation and Routing in WSN," *Journal of Information Security and Applications*, vol. 98, May 2026, Art. no. 104372, https://doi.org/10.1016/j.jisa.2026.104372.

[17] M. A. Khan *et al.*, "An Improvised Certificate-Based Proxy Signature Using Hyperelliptic Curve Cryptography for Secure UAV Communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 4, pp. 5264–5275, Apr. 2025, https://doi.org/10.1109/TITS.2024.3524575.

[18] M. Abu-Faraj, A. Al-Hyari, K. Aldebei, Z. A. Alqadi, and B. Al-Ahmad, "Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography," *IEEE Access*, vol. 10, pp. 69388–69397, 2022, https://doi.org/10.1109/ACCESS.2022.3187317.

[19] Y. Ma, J. Qiu, X. Sun, and Y. Tao, "A Novel Cryptography-Based Architecture to Achieve Secure Energy Trading in Microgrid," *IEEE Transactions on Smart Grid*, vol. 15, no. 2, pp. 2056–2072, Mar. 2024, https://doi.org/10.1109/TSG.2023.3294592.

[20] P. Radanliev, "Artificial Intelligence and Quantum Cryptography," *Journal of Analytical Science and Technology*, vol. 15, no. 1, Feb. 2024, Art. no. 4, https://doi.org/10.1186/s40543-024-00416-6.

[21] D. Ghosh, K. Ghosh, C. Chakraborty, A. Datta, and S. Gupta, "Securing the Future: Emerging Threats and Countermeasures in Cryptography," in *Securing the Digital Frontier*, 1st ed., K. Sharma, V. Sharma, P. Nand, A. K. Sagar, and G. Shrivastava, Eds. Hoboken, NJ, USA: Wiley, 2025, pp. 91–107.

[22] A. S. Ahanger, F. S. Masoodi, A. Khanam, and W. Ashraf, "Managing and Securing Information Storage in the Internet of Things," in *Internet of Things Vulnerabilities and Recovery Strategies*, 1st ed., New York City, NY, USA: Auerbach Publications, 2024, pp. 102–151.

[23] Y. M. Dalal, S. Supreeth, K. Amuthabala, T. Y. Satheesha, PN. Asha, and S. Somanath, "Optimizing Security: A Comparative Analysis of RSA, ECC, and DH Algorithms," in *2024 IEEE North Karnataka Subsection Flagship International Conference*, Bagalkote, India, Sep. 2024, pp. 1–6, https://doi.org/10.1109/NKCon62728.2024.10775183.

[24] N. Naveen and J. Nirmaladevi, "Secure Bio-Inspired Optimization with Intrusion Aware on-Demand Routing in MANETs," *Scientific Reports*, vol. 15, no. 1, Jul. 2025, Art. no. 25335, https://doi.org/10.1038/s41598-025-99269-1.

[25] M. Abudalou, "Enhancing Data Security through Advanced Cryptographic Techniques," *International Journal of Computer Science and Mobile Computing*, vol. 13, no. 1, pp. 88–92, Jan. 2024, https://doi.org/10.47760/ijcsmc.2024.v13i01.007.

[26] A. O. Ezeogu, "Post-Quantum Cryptography for Healthcare: Future-Proofing Population Health Databases Against Quantum Computing Threats," *Research Corridor Journal of Engineering Science*, vol. 2, no. 1, pp. 29–56, Feb. 2025, https://doi.org/10.66320/s0k5vw19.

[27] Z. Yu, "Research on Cryptography Based on Quantum-Resistant Algorithms," in *2024 International Conference on Electronics and Devices, Computational Science (ICEDCS)*, Sep. 2024, pp. 149–154, https://doi.org/10.1109/ICEDCS64328.2024.00031.

[28] S. N. Yusof, M. R. K. Ariffin, and W. N. Aqlili, "A Cryptanalysis on the Bivariate Cryptosystem in a Multivariate Setting," in *Cryptology and Information Security Conference*, Sep. 2024, Art. no. 75.

[29] A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra, and M. Liyanage, "Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography," in *2024 15th International Conference on Network of the Future*, Oct. 2024, pp. 195–203, https://doi.org/10.1109/NoF62948.2024.10741441.

[30] H. Y. Naser, A. K. Mattar, M. A. Saare, M. A. Almaiah, and R. Shehab, "A Comparison of Lightweight Cryptographic Protocols for Energy-Efficient and Sustainable IoMT Authentication," *Engineering, Technology & Applied Science Research*, vol. 15, no. 4, pp. 25746–25756, Aug. 2025, https://doi.org/10.48084/etasr.12204.

[31] "BOSS Base v1.0.1 Dataset." Binghamton, 2023, [Online]. Available: https://dde.binghamton.edu/download/.